



## UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

## NOTICE OF ALLOWANCE AND FEE(S) DUE

8968 7590 03/25/2010

DRINKER BIDDLE & REATH LLP  
ATTN: PATENT DOCKET DEPT.  
191 N. WACKER DRIVE, SUITE 3700  
CHICAGO, IL 60606

EXAMINER	
SU, SARAH	
ART UNIT	PAPER NUMBER
2431	
DATE MAILED: 03/25/2010	

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/519,698	12/27/2004	Marc Girault	P1907US	6941

TITLE OF INVENTION: CRYPTOGRAPHIC METHOD AND DEVICES FOR FACILITATING CALCULATIONS DURING TRANSACTIONS

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	\$1510	\$300	\$0	\$1810	06/25/2010

**THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.**

**THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.**

**HOW TO REPLY TO THIS NOTICE:**

I. Review the SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.

B. If the status above is to be removed, check box 5b on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above, or

If the SMALL ENTITY is shown as NO:

A. Pay TOTAL FEE(S) DUE shown above, or

B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check box 5a on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and 1/2 the ISSUE FEE shown above.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

**IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.**

## PART B - FEE(S) TRANSMITTAL

**Complete and send this form, together with applicable fee(s), to:** **Mail Stop ISSUE FEE**  
**Commissioner for Patents**  
**P.O. Box 1450**  
**Alexandria, Virginia 22313-1450**  
**or Fax (571)-273-2885**

**INSTRUCTIONS:** This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

8968            7590            03/25/2010

**DRINKER BIDDLE & REATH LLP**  
ATTN: PATENT DOCKET DEPT.  
191 N. WACKER DRIVE, SUITE 3700  
CHICAGO, IL 60606

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

### **Certificate of Mailing or Transmission**

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)

(Signature)

(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/519,698	12/27/2004	Marc Girault	P1907US	6941

TITLE OF INVENTION: CRYPTOGRAPHIC METHOD AND DEVICES FOR FACILITATING CALCULATIONS DURING TRANSACTIONS

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	\$1510	\$300	\$0	\$1810	06/25/2010
EXAMINER		ART UNIT	CLASS-SUBCLASS			
SU, SARAH		2431	380-282000			
1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).						
<input type="checkbox"/> Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.				1 _____		
<input type="checkbox"/> "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. <b>Use of a Customer Number is required.</b>				2 _____		
				3 _____		
3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)						

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent):  Individual  Corporation or other private group entity  Government

4a. The following fee(s) are submitted:

- Issue Fee
- Publication Fee (No small entity discount permitted)
- Advance Order - # of Copies \_\_\_\_\_

4b. Payment of Fee(s): (Please first reapply any previously paid issue fee shown above)

- A check is enclosed.
- Payment by credit card. Form PTO-2038 is attached.
- The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number \_\_\_\_\_ (enclose an extra copy of this form).

5. Change in Entity Status (from status indicated above)

- a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.
- b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature \_\_\_\_\_

Date \_\_\_\_\_

Typed or printed name \_\_\_\_\_

Registration No. \_\_\_\_\_

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/519,698	12/27/2004	Marc Girault	P1907US	6941
8968	7590	03/25/2010	EXAMINER	
DRINKER BIDDLE & REATH LLP ATTN: PATENT DOCKET DEPT. 191 N. WACKER DRIVE, SUITE 3700 CHICAGO, IL 60606				SU, SARAH
ART UNIT		PAPER NUMBER		
2431				DATE MAILED: 03/25/2010

## Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)

(application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 782 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 782 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (<http://pair.uspto.gov>).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

<b>Examiner-Initiated Interview Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	10/519,698	GIRAULT ET AL.	

  

<b>Examiner</b>	<b>Art Unit</b>	
Sarah Su	2431	

**All Participants:**

**Status of Application:** \_\_\_\_\_

(1) Sarah Su. (3) \_\_\_\_\_.

(2) Mark Bergner (45,877). (4) \_\_\_\_\_.

**Date of Interview:** 19 March 2010

**Time:** 10:00 AM

**Type of Interview:**

- Telephonic  
 Video Conference  
 Personal (Copy given to:  Applicant     Applicant's representative)

Exhibit Shown or Demonstrated:  Yes     No

If Yes, provide a brief description: \_\_\_\_\_.

**Part I.**

Rejection(s) discussed:

*none*

Claims discussed:

*Claims 1, 13, and 16 were discussed.*

Prior art documents discussed:

*none*

**Part II.**

SUBSTANCE OF INTERVIEW DESCRIBING THE GENERAL NATURE OF WHAT WAS DISCUSSED:

*See Continuation Sheet*

**Part III.**

- It is not necessary for applicant to provide a separate record of the substance of the interview, since the interview directly resulted in the allowance of the application. The examiner will provide a written summary of the substance of the interview in the Notice of Allowability.  
 It is not necessary for applicant to provide a separate record of the substance of the interview, since the interview did not result in resolution of all issues. A brief summary by the examiner appears in Part II above.

/Sarah Su/  
 Examiner, Art Unit 2431

(Applicant/Applicant's Representative Signature – if appropriate)

Continuation of Substance of Interview including description of the general nature of what was discussed: The applicant's representative has authorized an examiner's amendment to:

a. Cancel claims 5, 14, and 19.

b. In claim 1, line 5: delete "generating, at the first entity" and insert -generating, on a processor at the first entity-;

c. In claim 1, after line 15, insert:

"wherein the second element of proof is generated by the first entity by subtracting, from the random integer, the private key multiplied by the common number,

wherein the linear combination equal to the second exponent comprises a positive unitary coefficient for the common number and a positive unitary coefficient for the public key exponent multiplied by the second element of proof, and wherein, in the verified relationship, the first element of proof is considered with a unitary exponent power."

d. In claim 13, after line 15, insert:

"wherein the calculation means is designed to generate the second element of proof by taking the difference between the random integer and the private key multiplied by the common number or, where the common number is split into two elementary common numbers, by subtracting from the random integer multiplied by the first elementary common number, the private key multiplied by the second elementary common number."

e. In claim 15, line 1: delete "as claimed in claim 14" and insert –as claimed in claim 13–;

f. In claim 16, after line 14, insert:

"wherein the second element of proof is generated by the first entity by subtracting, from the random integer, the private key multiplied by the common number, wherein the linear combination equal to the second exponent comprises a positive unitary coefficient for the common number and a positive unitary coefficient for the public key exponent multiplied by the second element of proof, and wherein, in the verified relationship, the first element of proof is considered with a unitary exponent power."

g. In claim 20, line 1: delete "as claimed in claim 19" and insert –as claimed in claim 1–;

h. In claim 22, line 1: delete "as claimed in claim 19" and insert –as claimed in claim 1–;

i. In the Abstract, line 2: delete "means of a private RSA key" and insert –use of a private RSA key–;

j. In the Abstract, line 2: delete "means of a public RSA key" and insert –use of a public RSA key–.